L'influence de la cryptologie moderne sur les Mathématiques et l'Université

Jean-Louis Nicolas

In
Cryptologie et Mathématiques
Une mutation des enjeux,
Sous la direction de Marie-José Durand-Richard
et Philippe Guillot,
Collection Histoire des Sciences, Série Etudes,
L'Harmattan, Paris, 2014, 267-283.

L'INFLUENCE DE LA CRYPTOLOGIE MODERNE SUR LES MATHEMATIQUES ET L'UNIVERSITE

Jean-Louis NICOLAS[1]

INTRODUCTION

Le 20 juillet 1969, au moment où l'homme marchait pour la première fois sur la lune, se tenait à la State University of New-York at Stony Brooke l'école d'été de l'AMS (*American Mathematical Society*) « Summer School in Number Theory », consacrée à la théorie des nombres. Parmi les exposés prestigieux, il y avait celui de Daniel Shanks (1917-96), « Quadratic Forms » dont on trouvera la rédaction dans les Compte-rendus de cette école d'été[2].

Par le biais du calcul du nombre de classes $h(\Delta)$ des formes quadratiques primitives $ax^2 + bxy + cy^2$ (où a, b, c sont des nombres entiers avec $a > 0$, $c > 0$ et pgcd$(a, b, c) = 1$) de discriminant négatif $\Delta = b^2 - 4ac$ fixé[3], Shanks proposait une méthode de factorisation entièrement nouvelle, permettant de calculer les facteurs premiers des nombres ayant jusqu'à 30 ou 40 chiffres.

---

[1] jlnicola@in2p3.fr, Université de Lyon, Université Lyon1, CNRS. UMR 5208, Institut Camille Jordan Bât. Jean Braconnier, 21 Avenue Claude Bernard F-69622 Villeurbanne cedex, France. http://math.univ-lyon1.fr/~nicolas/.

[2] Shanks, « Class number, a theory of factorization, and *genera* ».

[3] On dit que la forme $f(x, y) = ax^2 + bxy + cy^2$ représente le nombre entier N s'il existe des nombres entiers x_0 et y_0 tels que $f(x_0, y_0) = N$. Sur l'ensemble $Q(\Delta)$ des formes quadratiques primitives de discriminant Δ, on définit une relation d'équivalence telle que deux formes équivalentes représentent les mêmes nombres. L'ensemble quotient $H(\Delta)$ de $Q(\Delta)$ par cette relation d'équivalence est un ensemble fini dont le cardinal est $h(\Delta)$. Gauss (voir *Disquisitiones Arithmeticae*) a défini une loi de composition de deux formes quadratiques f' et f'' de même discriminant ayant la propriété suivante : si f' représente N' et f'' représente N'', alors la composée de f' et f'' représente le produit $N'N''$.

En écoutant l'exposé de Shanks en 1969, je n'ai pas pleinement compris l'intérêt de son algorithme, tant il était éloigné des préoccupations habituelles des mathématiciens de cette époque.

Je suis maintenant de plus en plus persuadé que ce travail de Shanks a été une étape importante dans l'orientation des mathématiques vers les mathématiques effectives, c'est-à-dire les mathématiques ne se contentant pas de définir les objets, mais donnant des algorithmes, si possible rapides, permettant de les calculer.

Une décennie plus tard, l'année 1978 voyait la publication du protocole de cryptographie à clé publique RSA[4]. Ce protocole, basé sur la relative facilité à construire de grands nombres premiers et l'impossibilité de trouver les facteurs premiers de certains grands nombres composés, allait donner à cette orientation vers les mathématiques effectives un essor encore plus formidable.

Nous exposerons d'abord quelques signes de cette évolution des mathématiques. Puis, nous verrons comment s'est traduite cette évolution en termes d'enseignement avec la mise en place à Limoges, en 1985, du premier diplôme français axé sur la cryptologie. Actuellement de tels enseignements à bac + 5 existent à Bordeaux, Caen, Grenoble, Lyon, Marseille, Paris (École Polytechnique et École Normale Supérieure[5]), *etc.*

Les notions de mathématiques ou de cryptographie évoquées dans cet article sont supposées connues, au moins superficiellement, par le lecteur[6].

INFLUENCE DE LA CRYPTOLOGIE SUR LES MATHEMATIQUES

Les mathématiques avant 1978

Dans les années 1960, on n'enseignait guère l'histoire des mathématiques. Mis à part quelques exceptions (théorème de Pythagore,

---

[4] Du nom de ses trois inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman, « A method for obtaining digital signatures and public-key cryptosystems ». James Ellis avait découvert antérieurement la cryptographie à clé publique, sur laquelle il avait écrit en 1970 un rapport secret qui n'a été divulgué qu'en 1997. Voir par exemple http://fr.wikipedia.org/wiki/James_Ellis. W. Diffie et M. E. Hellman ont publié en 1976 un autre protocole de cryptographie à clé publique. Voir le chapitre « Les nouvelles orientations de la cryptographie » pp. 186-187, et le chapitre « Pourquoi et comment la cryptologie vient de surgir dans le domaine public », pp. 209-216.

[5] NdE. : Une telle formation existe aussi à l'Université Paris 8 Vincennes-Saint-Denis depuis 2003.

[6] Pour plus d'information, on pourra consulter les ouvrages suivants : Cohen, *A Course in Computational Algebraic Number Theory* ; Crandall et Pomerance, *Prime Numbers, a Computational Perspective* ; Menezes, Van Oorschot et Vanstone, *Handbook of Applied Cryptography*.

groupe de Galois, matrice de Jordan, somme de Darboux, théorème de Rolle, ...), on ne disait ni quand ni par qui avait été introduite une notion ou démontré un théorème.

Pour les objets introduits, on donnait en général une méthode de calcul dans les cas simples, mais on ne s'occupait pas d'évaluer cette méthode dans les cas plus compliqués. On apprenait ainsi à développer un déterminant d'ordre 3 par la règle de Sarrus ou à faire des combinaisons de lignes ou de colonnes pour calculer un déterminant d'ordre 4 ; mais on ne disait pas qu'un déterminant d'ordre n se calcule en $O(n^3)$ opérations par la méthode du pivot de Gauss, pourtant connue depuis longtemps.

Par l'algorithme d'Euclide, pour calculer le pgcd de deux nombres a_1 et a_2 (avec $a_1 > a_2$), pour $i = 3, 4, 5, \ldots$, on calcule a_i, le reste dans la division de a_{i-1} par a_{i-2} jusqu'à ce que a_i soit nul. Le pgcd de a_1 et a_2 est alors a_{i-1}. Combien de divisions faut-il exécuter lorsque les deux nombres initiaux a_1 et a_2 ont 100 chiffres décimaux ?

Cette question a été résolue par le théorème de Lamé (1845) qui démontre que, pour calculer le pgcd de deux nombres a_1 et a_2 avec $a_1 > a_2$, le nombre de divisions à effectuer est inférieur à 5 fois le nombre de chiffres décimaux de a_2.

Aucun professeur de mathématiques ne m'a enseigné le théorème de Lamé, que j'ai découvert dans le livre de Knuth[7]. Pourtant, Gabriel Lamé (1795-1870) est un mathématicien connu : il a résolu le cas de l'exposant 7 dans le grand théorème de Fermat en prouvant que l'équation $x^7 + y^7 = z^7$ n'a pas de solution entière vérifiant $xyz \neq 0$. Mais en 1960, les mathématiciens ne s'intéressaient que peu à l'évaluation des algorithmes, aux mathématiques effectives et aux ordinateurs[8].

Pourtant, il y avait des exceptions. Derrick Henry Lehmer (1905-91) connaissait[9] les méthodes de calcul rapide en arithmétique, en particulier l'évaluation de l'exponentielle modulaire ab mod N, et a effectué un énorme travail de calcul. La revue *Mathematics of Computation* lui a consacré un volume spécial en 1975, pour son soixante-dixième anniversaire[10]. Nous avons vu dans l'introduction que Daniel Shanks a découvert en 1969 une nouvelle méthode de factorisation. Arthur Oliver Lonsdale Atkin (1925-

---

[7] Knuth « The art of computer programming ».

[8] NdE. : Les recherches de Gabriel Lamé (1795-1870) ont été cependant effectuées dans un tout autre cadre. Lamé appartient à toute une génération de polytechniciens français qui ont développé une physique mathématique rationnelle. Menés en relation étroite avec l'étude des fonctions elliptiques, ses travaux sur les coordonnées curvilignes deviendront l'outil indispensable de la géométrie différentielle. Ils le conduiront à la théorie des nombres. Lamé est également connu pour son analyse de la complexité algorithmique de l'algorithme d'Euclide.

[9] Lehmer « Computer technology applied to the theory of numbers ». Voir le chapitre « Cryptographie et théorie des nombres » pp. 256-258.

[10] Collectif, « Special issues of mathematics of computation ».

2008) a utilisé les tout premiers ordinateurs et organisé le colloque *Computers in Number Theory* qui s'est tenu à Oxford[11] du 18 au 23 août 1969.

En France aussi, quelques mathématiciens commençaient à s'intéresser à ces questions ainsi qu'aux premiers logiciels de calcul formel ; citons notamment Maurice Mignotte à St-Denis[12] puis Strasbourg, Henri Cohen à Bordeaux et Grenoble, Georges et Marie-Nicole Gras à Grenoble puis Besançon. On lira en annexe l'échange de lettres en 1974 avec le grand informaticien Marcel-Paul Schützenberger (1920-96) sur la mise en place d'un centre de calcul spécialisé en arithmétique. Le colloque « Utilisation des ordinateurs en Mathématiques » a réuni à Limoges en septembre 1975 un ensemble de mathématiciens prêts à s'investir dans ces sujets[13].

En conclusion, on voit qu'il existait autour de l'utilisation des ordinateurs en théorie des nombres et du calcul formel un bouillonnement d'idées qui sera largement amplifié par la découverte de la cryptographie à clé publique. Le développement des logiciels de calcul formel Pari/GP, Sage, Magma, Maple, *etc.* en a grandement profité.

Questions développées sous l'influence de la cryptologie

Le protocole de cryptographie RSA et celui du logarithme discret font jouer un grand rôle aux nombres premiers et à la décomposition en facteurs premiers des nombres composés[14].

Un *test de primalité* prend en entrée un nombre N et, en sortie, déclare si le nombre est premier ou composé. Un *algorithme de factorisation* prend en entrée un nombre N garanti composé par un test de primalité et donne en sortie deux nombres différents de 1 dont le produit vaut N.

La méthode dite des divisions successives, qui consiste à diviser N par les nombres premiers inférieurs ou égaux à $\sqrt{N}$, est à la fois un test de primalité et un algorithme de factorisation. Mais la plupart des algorithmes de factorisation énumérés ci-après ne prouvent pas qu'un nombre est premier.

Plusieurs tests de primalité et algorithmes de factorisation ont été découverts dans les années 1970, mais il faudra attendre les années 1980 pour voir apparaître les algorithmes les plus efficaces.

---

[11] Ed. Atkin et Birch, *Computers in number theory*.

[12] NdE. : Maurice Mignotte a d'abord enseigné à l'université Paris XIII, qui avait une antenne dans la ville de Saint-Denis.

[13] Collectif, « Utilisation des ordinateurs en mathématiques ».

[14] Voir les chapitres « Nouvelles orientations de la cryptographie » p. 173 et « Pourquoi et comment la cryptographie vient de surgir dans le domaine public ? » p. 203.

Tests de primalité

La méthode des divisions successives est connue depuis l'Antiquité ; en dehors de la méthode $N-1$ introduite par Édouard Lucas (1842-91) à la fin du 19e siècle[15], les autres méthodes décrites ci-dessous sont postérieures à 1970.

Méthode $N-1$ ou $N+1$. Elle permet de tester la primalité du nombre N lorsque l'on connait les facteurs premiers de $N-1$ ou de $N+1$.

Test probabiliste d'Artjuhov-Miller-Rabin. Ce test dit qu'un nombre est premier avec une très forte probabilité[16]. Cependant, il ne garantit pas que le nombre testé soit premier. Mais il est rapide et il faut l'utiliser avant d'appliquer l'un des tests non probabilistes cités ci-dessous.

Test probabiliste des suites de Lucas. Les suites de Lucas sont les suites récurrentes linéaires d'ordre 2, c'est-à-dire définies par leurs deux premiers termes x_0 et x_1 et par la relation de récurrence $x_{n+2} = ax_{n+1}+bx_n$. La plus célèbre est la suite de Fibonacci, avec $x_0 = 0$, $x_1 = 1$, $a = 1$, $b = 1$. Ces suites permettent de construire un test probabiliste qui, comme le test d'Artjuhov-Miller-Rabin, est rapide mais ne permet pas de garantir la primalité du nombre testé.

Test des sommes de Jacobi. Ce test a été publié en 1983 par Adleman, Pomerance et Rumely puis implémenté par Cohen et Lenstra[17]. Le temps nécessaire à prouver la primalité du nombre N est $O((\log N)^{\log\log\log N})$, ce qui est presque polynomial en $\log N$.

Test utilisant les courbes elliptiques. Shafi Goldwasser[18] et Joe Kilian ont publié en 1986 un premier test théorique. Le test ECPP (Elliptic Curve Primality Proving) publié par Atkin et Morain[19] en 1993 permet de tester de grands nombres au hasard[20]. En décembre 2012, le teste CIDE (*Cyclotomy Initialized by Dual Elliptic tests*) de Pedra Mihailescu a permis à Jens Franke, Thorsen Kleinjung, Andreas Decker et Anna Grosswendt de prouver la primalité du nombre de 30 008 chiffres : $8656^{2929} + 2929^{8656}$, ce qui est le record actuel pour un nombre « au hasard ».

Test AKS (Agrawal, Kayal, Saxena). Cet algorithme, publié en 2004, montre que l'on peut tester la primalité de N en $O((\log N)^c)$ étapes, autrement dit, que ce test est polynomial en $\log N$. Malheureusement,

---

[15] Voir le chapitre « Cryptographie et théorie des nombres » pp. 258-259.

[16] Voir plus loin le paragraphe « Nombres premiers avec une grande probabilité ».

[17] Voir le chapitre « Pourquoi et comment la cryptologie vient de surgir dans le domaine public ? » p. 214.

[18] *ibid.*, p. 217.

[19] Atkin et Morain, « Elliptic curves and primality proving » ; « Finding suitable curves ».

[20] Par le test ECPP, le nombre « au hasard » de 20 562 chiffres décimaux :
$(((((((((2^3 + 3)^3 + 30)^3 + 6)^3 + 80)^3 + 12)^3 + 450)^3 + 894)^3 + 3636)^3 + 70756)^3 + 97220$ a été prouvé premier en 2006, voir http://primes.utm.edu.

jusqu'à maintenant, cette vitesse n'est que théorique ; aucune version implémentée ne permet de rivaliser avec les deux précédents tests.

Méthodes de factorisation

CFRAC. Très peu de temps après la méthode de factorisation de Shanks (1969) apparaissait un autre algorithme de factorisation, la méthode CFRAC utilisant les fractions continues[21], qui donnait les deux facteurs premiers du nombre de Fermat $F_7 = 2^{128} + 1$, un nombre de 39 chiffres.

CLASSNO et SQUFOF. Après avoir publié son premier algorithme de factorisation CLASSNO[22], Shanks en découvrit un deuxième, SQUFOF, utilisant les formes quadratiques, cette fois à discriminant négatif. L'algorithme peut se programmer en peu d'instructions et travaille essentiellement sur des nombres dont le nombre de chiffres est inférieur à la moitié du nombre de chiffres du nombre à factoriser. En 1973, sont apparues les premières calculettes programmables, et l'algorithme SQUFOF implémenté sur ces machines, permettait de factoriser des nombres de 18 chiffres décimaux[23].

Algorithme de Lehman. Factoriser un nombre impair sous la forme $N = a \times b$ est équivalent à l'écrire sous forme d'une différence de deux carrés $N = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$. Par cette observation, Fermat avait trouvé une méthode simple pour décomposer en facteurs premiers les nombres qui ont deux facteurs voisins de $\sqrt{N}$. En améliorant la technique de Fermat, Sherman Lehman a obtenu un algorithme de factorisation (qui est aussi un test de primalité) en $O(N^{1/3})$.

La méthode p de Pollard. C'est un algorithme probabiliste, basé sur le paradoxe des anniversaires, très simple à programmer, dont le temps de calcul est $O(N^{1/4})$.

Les méthodes p − 1 et p + 1 de Pollard. Ces méthodes permettent de trouver les facteurs premiers p d'un nombre N tels que $p - 1$ (ou $p + 1$) n'ait que des petits facteurs premiers.

Le crible quadratique. Pour factoriser N, on considère le polynôme $P(x) = \left(x + \left\lfloor \sqrt{N} \right\rfloor\right)^2 - N$, et l'on recherche les petites valeurs de x telles que $P(x)$ soit friable, c'est-à-dire n'ait que des petits facteurs premiers. Cette recherche peut se faire rapidement par une technique de crible. Cet algorithme, publié en 1982 par Carl Pomerance (né en 1944), a permis en

---

[21] Morisson et Brillhart, « The Factorization of F_7 », « A Method of Factoring and the Factorization of F_7 ».
[22] Shanks, « Class Number, a Theory of Factorization ».
[23] Nicolas, « Une méthode de factorisation ».

1983 de factoriser le nombre $(10^{71} - 1)/9$ qui s'écrit avec 71 chiffres 1. La méthode MPQS (*Multiple Polynomial Quadratic Sieve*) remplace le polynôme $P(x)$ par d'autres polynômes du second degré.

L'algorithme ECM (Elliptic Curve Method). Soit p un facteur premier inconnu du nombre N à factoriser. On choisit au hasard une courbe elliptique $y^2 = x^3 + ax + b$, en espérant que son nombre de points sur le corps $\mathbb{F}_p$ soit friable, c'est-à-dire n'ait que des petits facteurs premiers. Cet algorithme a été publié en 1987 par Hendrik Lenstra Jr[24].

Le crible du corps de nombres. C'est actuellement la méthode la plus performante. Elle travaille à la fois dans le corps $\mathbb{Q}$ des nombres rationnels et dans un corps de nombres $\mathbb{Q}(\theta)$, où θ est un nombre algébrique bien choisi. La version initiale, suggérée par John Pollard en 1988, permettait de factoriser les nombres de la forme $a^n + b^n$, par exemple les nombres de Mersenne[25] ou de Fermat[26]. Généralisée aux nombres quelconques, cette méthode a permis la factorisation d'un nombre de 232 chiffres, ce qui est le record actuel. On lira avec intérêt l'article de Pomerance sur ce sujet[27].

En conclusion, on constate la variété des domaines mathématiques intervenant dans ces différents algorithmes de factorisation. Enfin, rappelons que si les ordinateurs quantiques fonctionnent un jour, ils résoudront rapidement le problème de factorisation.

Théorie de la complexité

Le principe du protocole de cryptographie RSA est basé sur la possibilité de construire de grands nombres premiers p et q (de, disons, 150 chiffres) et sur l'impossibilité actuelle de retrouver les facteurs premiers p et q à partir de leur produit (la fonction : $(p, q) \rightarrow p \times q$ est une fonction à sens unique[28]).

Mais cette impossibilité est-elle inhérente au problème ou bien est-elle due à notre ignorance actuelle ? Nous avons vu dans les tests de primalité que la méthode AKS testait la primalité d'un nombre N en temps polynomial par rapport au nombre de chiffres de N. Existe-t-il un algorithme polynomial de factorisation ?

En théorie de la complexité, la classe ***P*** réunit les problèmes qui peuvent être décidés en temps polynomial par rapport à la taille des données. Par l'algorithme AKS, le problème de primalité appartient à la classe ***P***. La

---

[24] Lenstra, « Factoring integers with elliptic curves ».
[25] Voir la note 28, p. 235.**Erreur ! Source du renvoi introuvable.**
[26] Voir page précédente.
[27] Pomerance, « A tale of two sieves ».
[28] Voir le chapitre « Les nouvelles orientations de la cryptographie » pp. 196-199, et plus loin le paragraphe « Fonctions à sens unique ».

classe ***NP*** contient les problèmes de décision qui admettent un algorithme polynomial capable de tester la validité d'une de leurs solutions. Le problème de factorisation appartient à la classe ***NP***. La fameuse conjecture[29] ***P*** = ***NP*** entraînerait que le problème de factorisation est dans la classe ***P*** et donc il existerait un algorithme de factorisation polynomial en le nombre de chiffres de l'entrée N.

Pour rendre le protocole RSA caduc, encore faudrait-il qu'un tel algorithme de factorisation soit performant en pratique.

Courbes elliptiques

Les courbes elliptiques sont les courbes les plus simples après les droites et les coniques. On peut ramener leur équation à la forme de Weierstrass :

$$y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0.$$

Sur une telle courbe on définit l'addition de deux points. L'élément neutre 0 de cette addition est le point à l'infini dans la direction $[Oy)$, et trois points alignés ont pour somme 0. L'ensemble des points de la courbe muni de cette opération est un groupe abélien.

On peut considérer une courbe elliptique sur un corps fini, par exemple $\mathbb{F}_p$. C'est de cette façon que les courbes elliptiques interviennent dans les tests de primalité, dans la méthode de factorisation ECM et dans certains protocoles de cryptographie. Cela a suscité de nombreux travaux, par exemple sur le calcul du nombre de points d'une courbe elliptique sur un corps fini de grande taille.

L'algorithme LLL

Cet algorithme a été publié en 1982 par Henrik Lenstra, Arjen K. Lenstra et László Lovász pour trouver les facteurs irréductibles d'un polynôme à coefficients entiers. Depuis, il est devenu un outil incontournable tant en théorie algébrique des nombres qu'en cryptographie.

[29] Smale, « Mathematical problems for the next century ».

Quelques nouveaux concepts

Nombre premier avec « grande probabilité »

Le petit théorème de Fermat[30] affirme que, si p est un nombre premier, $2^{p-1} - 1$ est multiple de p. La réciproque n'est pas vraie ; il existe une infinité de nombres N composés, appelés pseudo-premiers en base 2, qui vérifient :

$$2^{N-1} - 1 \equiv 1 \pmod{N}. \tag{1}$$

Le plus petit est $341 = 11 \times 31$. Mais ces nombres sont très rares, et si le nombre N vérifie la congruence (1), on peut parier, avec de grandes chances de gagner, qu'il est premier.

Le test d'Artjuhov-Miller-Rabin est une condition nécessaire de primalité encore plus forte que le test donné par l'équation (1). Cohen dit qu'un nombre N qui passe le test d'Artjuhov-Miller-Rabin est un nombre premier de qualité industrielle : si l'on utilise un tel nombre dans la construction d'un protocole de cryptographie, la probabilité que ce nombre soit composé est beaucoup plus faible que la probabilité d'une erreur humaine dans la gestion de ce protocole.

Mais pour un mathématicien, un nombre est premier ou il ne l'est pas, et cette notion de nombre premier avec grande probabilité engendrée par les tests probabilistes a suscité de nombreuses discussions.

Certificat de primalité

Il est facile de vérifier le résultat d'un algorithme de factorisation qui annonce d comme diviseur de N : il suffit de calculer le reste dans la division de N par d, et de constater que ce reste est nul. La plupart des algorithmes cités dans les méthodes de factorisation s'appuient sur des raisonnements heuristiques et probabilistes, mais leur temps de calcul est non prouvé ; cependant en pratique, ils fonctionnent. Le cas des tests de primalité est très différent. Que penser d'un algorithme qui, après des heures de calcul, déclare « N est premier » ou « N est composé » ?

Il peut y avoir une erreur. Un certificat de primalité est un ensemble de données qui permet de vérifier que le nombre est bien premier. La méthode des divisions successives n'a pas de certificat de primalité.

La méthode $N - 1$ des tests de primalité donne comme certificat la liste des facteurs premiers de $N - 1$ accompagnés de leur certificat de primalité.

---

[30] Voir le chapitre « Cryptographie et théorie des nombres » pp. 255-258.

Les tests ECPP et CIDE admettent un certificat de primalité, mais pas le test des sommes de Jacobi.

Fonctions « à sens unique »[31]

Soit p et q deux nombres premiers; il est facile (c'est un problème de la classe $\boldsymbol{P}$)[32] de calculer le produit $N = p \times q$. Réciproquement, les mathématiques disent que N est un produit de facteurs premiers, mais il est difficile de calculer p et q à partir de N, c'est un problème de la classe $\boldsymbol{NP}$. On dit que l'application : $(p, q) \longrightarrow N = p \times q$ est une fonction à sens unique. Chaque protocole de cryptographie à clé publique est basé sur une fonction à sens unique. L'application : $(p, q) \longrightarrow N$ est à la base du protocole RSA.

Soit p un nombre premier. Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, c'est-à-dire qu'il existe un générateur g tel que les deux ensembles $\{1, 2, \ldots, p-1\}$ et $\{g \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p = 1\}$ coïncident. L'application : $a \longrightarrow g^a \bmod p$ est une permutation de l'ensemble $\{1, 2, \ldots, p-1\}$. Par exemple, 3 est un générateur de $(\mathbb{Z}/7\mathbb{Z})^\times$; les puissances de 3 modulo 7 sont 3, 2, 6, 4, 5, 1. À partir de a, le calcul de $x = g^a \bmod p$ est facile par l'algorithme des puissances. Mais, à partir de x, le calcul de a, appelé logarithme discret de x en base g, est en général plus compliqué. Nous avons là encore une fonction à sens unique.

La fonction à sens unique du logarithme discret existe aussi dans le groupe des éléments non nuls d'un corps fini (où p est premier) ainsi que dans le groupe des points d'une courbe elliptique sur un corps fini. Ces groupes sont utilisés en cryptographie.

Zéro connaissance[33]

Comment Alice peut-elle prouver à Bob qu'elle connaît un secret sans rien révéler de ce secret ? Cette situation se présente si Bob est le banquier d'Alice et si Alice veut retirer de l'argent à sa banque. Elle ne veut pas donner son secret à Bob pour ne pas risquer d'être escroquée, si celui-ci est malhonnête.

Alice doit fournir à Bob une preuve à divulgation nulle de connaissance. On trouvera sur le site http://fr.wikipedia.org/wiki/Preuve_ à_divulgation_ nulle_de_connaissance un schéma simple d'une telle preuve.

---

[31] Voir le chapitre « Les nouvelles orientations de la cryptographie » pp. 188-191.

[32] Voir plus haut le paragraphe « Théorie de la complexité ».

[33] Voir le chapitre « Pourquoi et comment la cryptologie a envahi le domaine public ? » pp. 217-225.

Le mathématicien et le cryptographe

Neal Koblitz est un mathématicien qui a suivi de près les mathématiques et leur rapprochement avec la cryptographie. Il a écrit plusieurs ouvrages sur le sujet[34].

Dans l'excellent article « The uneasy relationship between mathematics and cryptography » [35], il compare les méthodes de travail du cryptographe et du mathématicien. Le mathématicien, et particulièrement le théoricien des nombres, s'attaque à un problème ouvert, souvent ancien, et dans le meilleur des cas, le résout, mais, plus fréquemment, apporte une contribution positive en direction de la solution. Le cryptographe, comme le biologiste ou l'informaticien, est pris dans la spirale du temps et prépare activement sa présentation au prochain congrès, quelquefois aux dépens d'une réflexion approfondie.

Je recopie ci-dessous les dernières lignes de cet article :

> « *Cryptography has the excitement of being more than just an academic field. Once I heard a speaker of NSA complain about university researchers who are cavalier about proposing untested cryptosystems. He pointed out that in the real world if your cryptography fails, you lose a million dollars or your secret agent gets killed. In academia, if you write about a cryptosystem and then a few months later find a way to break it, you've got two new papers to add to your résumé!*
> *Drama and conflict are inherent in cryptography, which, in fact can be defined as the science of transmitting and managing information in the presence of an adversary. The "spy* vs. *spy" mentality of constant competition and rivalry extends to the disciplinary culture of the field. This can get to be excessive – and even childish at times – but it also explains in part why it can be so much fun to do research in cryptography* ».

Il est sans doute bon d'avoir un regard sur les applications immédiates, sans perdre de vue les grands objectifs qui permettent les avancées de la Science. On notera que, dans les universités, la cryptographie est enseignée, tantôt en mathématiques, tantôt en informatique.

---

[34] Par exemple Koblitz, *A course in number theory and cryptography*.

[35] Cet article est traduit au chapitre « La relation agitée entre mathématiques et cryptographie » pp. 285-303.

INFLUENCE DE LA CRYPTOLOGIE SUR L'UNIVERSITE

Création du DEA de Limoges

Au début des années 1980, il n'y avait pas d'enseignement de troisième cycle en mathématiques à l'Université de Limoges. Pourtant, le département de mathématiques, avec une trentaine d'enseignants, en avait le potentiel ; mais le MEN (Ministère de l'Éducation Nationale) ne souhaitait pas augmenter le nombre d'universités habilitées à délivrer un diplôme de troisième cycle. Il fallait donc trouver une idée un peu originale pour avoir quelques chances d'obtenir une habilitation.

Or, au printemps 1984, Pomerance a passé trois mois comme professeur invité à Limoges. De plus, le congrès *Eurocrypt*, qui avait eu lieu en 1982 à Burg Feuerstein[36] (Allemagne) et à Udine (Italie) en 1983, se tenait à la Sorbonne en mai 1984, et, pour la première fois, sous les hospices de l'IACR (*International Association of Cryptology Research*). À l'automne 1984, au moment de préparer les dossiers de demande de création de nouvelles filières, les enseignants limougeauds se dirent que la cryptographie pourrait être un atout.

Il n'était pas clair, à cette époque, de prévoir combien d'étudiants pourraient trouver un emploi dans la cryptographie. À côté de l'équipe de recherche en théorie des nombres, calcul formel et cryptographie, il y avait une équipe d'analyse numérique, spécialisée dans les problèmes d'optimisation. Il nous a semblé qu'une formation à Bac + 5, donnant aux étudiants les notions de base dans les domaines de ces deux équipes et accompagnée d'une bonne pratique de l'informatique ainsi que d'un stage en entreprise devrait permettre à ces étudiants d'obtenir un travail intéressant. La branche « Cryptographie » de Thomson-CSF (maintenant THALES) promettait d'accueillir nos étudiants en stage.

C'est sur ce schéma que fût adressée au Ministère de l'Éducation Nationale la demande de création du DEA[37] de mathématiques avec la mention « Cryptographie et Optimisation ». Dans la commission d'étude des dossiers, il y avait Jean-Louis Stehlé, qui travaillait alors chez IBM, et qui a fortement soutenu notre dossier ; finalement, ce DEA fût habilité.

Il semble que c'était la première fois qu'un enseignement de cryptographie se faisait en dehors d'un établissement militaire. Je me rappelle avoir envoyé au Service du Chiffre le programme détaillé de chacun des modules de ce DEA.

---

[36] Voir le chapitre « Cryptographie et théorie des nombres » p. 252.

[37] Diplôme d'Études Approfondies. Cet enseignement à Bac + 5 correspond maintenant à la deuxième année de Master.

Les premiers cours eurent lieu à l'automne 1985. Dans les deux premières promotions il y eut comme étudiant François Morain, actuellement professeur à l'École Polytechnique et Thierry Berger maintenant professeur à l'Université de Limoges.

En 2012-2013, la cryptologie continue d'être enseignée à l'Université de Limoges[38].

Influence sur la Recherche

En juillet 1988, l'AMS (*American Mathematical Society*) organisait dans le Maine un colloque présidé par Pomerance sur le sujet « Computational Number Theory »[39]. Daniel Barsky, qui présidait alors la commission du CNRS, favorisa la mise en place d'un PICS (Projet International de Coopération Scientifique) du CNRS avec les États-Unis qui permit de financer le voyage d'une vingtaine de mathématiciens français pour participer à ce colloque.

Peu après, sous la direction de Jacques Martinet, se créait à Bordeaux le laboratoire A2X (Équipe de Théorie des Nombres et d'Algorithmique Arithmétique), qui officialisait le travail important accompli par plusieurs mathématiciens bordelais dans l'utilisation des ordinateurs en théorie des nombres. Ce laboratoire s'est naturellement ouvert vers la théorie des codes et la cryptographie ; en particulier, les questions développées sous l'influence de la cryptologie y ont fait l'objet d'études fructueuses et tout laisse à penser que ces recherches ne s'arrêteront pas de sitôt.

Le DESS de Lyon

Nommé à Lyon en octobre 1988, je souhaitais y introduire un enseignement de cryptologie. Justement, l'Université Claude Bernard (Lyon 1) mettait en place à la rentrée 1989 un DESS[40] d'Ingénierie mathématique. Il comprenait un tronc commun et trois options, Analyse Numérique, Statistiques et Finances.

Dans le tronc commun, il y avait une initiation à la cryptographie et aux mathématiques sous-jacentes. Trois ans plus tard, s'ouvrit une quatrième option, Mathématiques Discrètes, qui recrutait plus particulièrement des étudiants de la Maîtrise de Mathématiques Discrètes, et qui incluait un

---

[38] Voir le site http ://www.cryptis.fr.

[39] Collectif, « Joint Summer Research Conference ».

[40] Diplôme d'Études Supérieures Spécialisées. Comme le DEA, cet enseignement à Bac + 5 correspond maintenant à la deuxième année de Master.

enseignement complémentaire de cryptographie. Plusieurs étudiants de cette option ont fait leur stage en entreprise dans le domaine de la cryptographie.

Au moment de la mise en place des Masters, les enseignements de cryptographie de ce DESS ont été transférés en deuxième année du Master de Lyon, mention Mathématiques et applications, Ingénierie mathématique et y sont encore en place[41] en 2012-2013.

BIBLIOGRAPHIE

Atkin, A. O. L. et Morain, F., « Finding Suitable Curves for the Elliptic Curve Method of Factorization ». *Mathematics of Computation*, 1993, vol. 60, pp. 399-405

— « Elliptic Curves and Primality Proving ». *Mathematics of Computation*, 1993, vol. 61, pp. 29-68.

(eds.) Atkin A. O. L. et Birch B. J., « Computers in Number Theory ». *Proceedings of the Science Research Council Atlas Symposium n°. 2*, held at Oxford, from 18-23 August 1969, Londres, New-York, Academic Press, 1971.

Collectif, « Special Issue of Mathematics of Computation dedicated to D. H. Lehmer », *Mathematics of Computation*, 1975, vol. 29.

Collectif, « Utilisation des ordinateurs en mathématiques, Colloque de Limoges, septembre 1975 », *Bulletin de la Société Mathématique de France*, 1977, Mémoire 49-50.

Collectif, « Joint Summer Research Conferences in the Mathematical Sciences », Bowdoin College, Brunswick, Maine, July 9 to July 15, *Computational Number Theory*, Notices of the American Mathematical Society, 1987, n° 34, pp. 1134-1135.

Cohen, H., *A course in Computational Algebraic Number Theory*. Graduate texts in Mathematics n° 138, Berlin, Springer Verlag, 1993.

Crandall, R. et Pomerance, C., *Prime Numbers, A Computational Perspective*, Berlin, Springer Verlag, 2001.

Gauss, C. F., *Disquisitiones Arithmeticae*, Traduit et prefacé par A. A. Clarke, révisé par W. C. Waterhouse, C. Greithe et A. W. Grootendorst New York, Springer Verlag, 1986.

Knuth, D. E., *The Art of Computer Programming*, vol. 2, *Seminumerical Algorithm*. New York, Addison-Wesley, 1981, 2e édition.

Koblitz, N., *A course in number theory and cryptography*, Graduate Texts in Mathematics, vol. 114. New York, Springer Verlag, 1987.

[41] Voir le site http://mastermath.univ-lyon1.fr.

— « The Uneasy Relationship between Mathematics and Cryptography », *Notices of the A.M.S.*, 2007, vol. 54, pp. 972-979.

Lehmer, D. H., « Computer Technology Applied to the Theory of Numbers ». *in* (éd.) W. J. Leveque, *Studies in Number Theory*, Washington D. C. Mathematical Association of America, 1969, pp. 117-151.

Lenstra, H., « Factoring integers with elliptic curves », *Annals of Mathematics*, 1987, 2nd series, vol. 126, n° 3, pp. 649-673.

Menezes, A. J., van Oorschot, P. C. et Vanstone, S. A., *Handbook of Applied Cryptography*, Boca Raton, CRC Press, 1997.

Morrison, M. A. et Brillhart, J., « The Factorization of F_7 », *Bulletin of the American Mathematical Society*, 1971, vol. 77, n° 2, pp. 264-264.

— « A Method of Factoring and the Factorization of F_7 », *Mathematics of Computation*, 1975, vol. 28, n° 129, pp. 183-205.

Nicolas. J.-L. « Une méthode de factorisation utilisant les formes quadratiques à discriminant positif », *L'Iremois, publication de l'IREM de Limoges*, 1981, n° 6, pp. 3-12.

Pomerance, C., « A tale of two sieves », *Notices of the American Mathematical Society*, 1996, vol. 43, n° 12, pp. 1473-1485.

Rivest, R. L., Shamir, A. et Adleman, L., « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems », *Communications of the Association for Computing Machinery*, 1978, vol. 21, n° 2, pp. 120-126.

Shanks, D., « Class Number, a Theory of Factorization, and Genera », 1969, Number Theory Institute, Stony Brooke, N. Y., *Proceeding of the Symposium on Pure Mathematics*, American Mathematical Society, 1971, vol. 20, pp. 415-440.

Smale. S. « Mathematical Problems for the Next Century ». *The Mathematical Intelligencer*, 1998, vol. 20, n° 2, pp. 7-15. Traduction *in* « Problèmes mathématiques pour le prochain siècle », *Gazette de la Société Mathématique de France*, 2000, n° 83, pp. 11-27.

ANNEXE

Lettre de J.-L. Nicolas à M.-P. Schützenberger[42]

Limoges, le 2 mai 1974,

Cher Monsieur,

Je vous envoie le menu des prochaines journées arithmétiques (27 mai – 1er juin) à Bordeaux. J'ai écrit à P. Damey, organisateur, pour qu'il vous envoie les renseignements techniques. Avec quelques autres arithméticiens qui s'intéressent aux calculs sur ordinateur (dont Mignotte de Paris XIII = St Denis), nous souhaiterions organiser quelque chose comme un centre de calcul spécialisé (au moins en partie) en arithmétique. L'idée est vaste et peu précise et je voudrais profiter des journées de Bordeaux pour la préciser. Vous avez sûrement des idées intéressantes sur ce sujet et vous connaissez plusieurs personnes qui en ont aussi. C'est une raison de plus d'espérer votre venue à Bordeaux.

Avec mes meilleurs sentiments,

J.-L. Nicolas

[42] Voir note p. 43, p. 261.

Lettre de M.-P. Schützenberger à
J.-L. Nicolas

Jeudi

Cher ami,

Merci de votre retransmission.

J'aimerais avoir plus de détail sur la réunion de Bordeaux où je voudrais beaucoup avoir la possibilité de venir

Peut-être que nous nous y rencontrerons

Amitié

M-P Schützenb-

97 rue du Ranelagh-
Paris XVI
647-67-02.